UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/586,671	06/01/2000	Igor Muttik	NA99-08101	5923

28875 7590 10/01/2004

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
PHAN, THAI Q	

ART UNIT	PAPER NUMBER
2128	

DATE MAILED: 10/01/2004

4

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/586,671	MUTTIK ET AL.	
	Examiner	Art Unit	
	Thai Q. Phan	2128	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 June 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to patent application S/N: 09/586,671, filed on June 01, 2000. Claims 1-36 are pending in the action.

Drawings

Formal drawings filed on 06/01/2000 are acceptable for examination.

Claim Rejections - 35 USC § 112

Claims 1-36 are rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. The present application discloses a plurality of emulation extensions but does not provide a clear description for emulation extension. What is the emulation extension in the present context? Why the emulation extension need, and how the extensions relate to the emulator. Such features are critical and essential to the practice of the invention to make the disclosure enable.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bond et al, US patent no. 6,275,938 B1.

As per claim 1, Bond discloses a method and system for security enhancement of untrusted code execution with feature limitations very similar to the claimed invention.

According to Bond, the method for enhancement of security of suspect code execution includes steps

Receiving the suspect code for execution (col. 5, lines 5-33

Loading the suspect code into an emulation buffer (Fig. 4) within a data space of a computer system,

Loading a first emulation extension into the emulator, wherein the emulator extension including program instruction to emulate suspect code in order to detect a computer virus or malicious software (col. 6, lines 24-52),

Performing an emulation using the first emulation extension and the suspect code, the emulation being performed within an insulated environment in the computer system (Figs 2, 3, col. 6, line 53 to col. 7, line 5) so that the computer system is insulated from malicious actions of the suspect code, and detecting and preventing the system from executing programs containing untrusted code (Field of the Invention). Bond does not expressly disclose the claimed feature of exhibit malicious behavior of the suspect code execution.

It would have been obvious for those skilled in the art at the time of the invention was made to realize the security enhancement in Bond above implies the claimed feature of malicious behaviour because the security program in Bond is to enhance security for program execution by preventing security breaches (col. 2, lines 7-14, for example) or uncertainty provenance or effects (col. 4, lines 54-57) due to execution of untrusted codes. In other words, the security enhancement program in Bond is to detect malicious behavior of the suspect code execution in the system.

As per claims 2 and 4, Bond discloses step of performing the emulation includes emulating the program instructions that comprise the emulation extension.

As per claim 3, due to the similarity of claim 3 to claim 1 above, and the security enhancement in Bond above implies the claimed feature of malicious behaviour because the security program in Bond is to enhance program execution by preventing security breaches (col. 2, lines 7-14, for example) or uncertainty provenance or effects (col. 4, lines 54-57). In other words, the security enhancement program in Bond is to detect malicious behavior of the suspect code execution in the system.

As per claim 5, Bond discloses emulating the suspect code prior to loading the emulation extension into the emulator buffer (col. 4, lines 39-57, col. 5, lines 23-33).

As per claim 6, Bond discloses the claimed limitations for detecting and preventing malicious codes or security breach in execution of the suspect code.

As per claim 7, Bond discloses a plurality of emulation extension for detecting malicious or virus code. This would imply the claimed limitation of resolving conflict.

As per claims 8-12, Bond discloses the claimed limitations for detecting and preventing malicious codes or security breach to resolve conflict and uncertainty provenance of program execution.

As per claim 13, Bond discloses a method, a system and a computer readable medium storing instructions for enhancing security of suspect code execution or untrusted executable code with feature limitations very similar to the claimed invention. According to Bond, the computer readable medium for enhancement of code execution includes means for performing steps

Receiving the suspect code for execution (col. 5, lines 5-33

Means for loading the suspect code into an emulation buffer (Fig. 4) within a data space of a computer system,

Loading a first emulation extension into the emulator, wherein the emulator extension including program instruction to emulate suspect code in order to detect a computer virus or malicious software (col. 6, lines 24-52),

Performing an emulation using the first emulation extension and the suspect code, the emulation being performed within an insulated environment in the computer system (Figs 2, 3, col. 6, line 53 to col. 7, line 5) so that the computer system is insulated from malicious actions of the suspect code, and detecting and preventing the system from executing programs containing untrusted code (Field of the Invention). Bond does not expressly disclose the claimed feature of exhibit malicious behavior of the suspect code execution.

It would have been obvious for those skilled in the art at the time of the invention was made to realize the security enhancement in Bond above implies the claimed feature of malicious behaviour because the security program in Bond is to enhance program execution by preventing security breaches (col. 2, lines 7-14, for example). In other words, the security enhancement program in Bond is to detect and prevent malicious behavior of the suspect code execution in the system.

As per claims 14 and 16, Bond discloses step of performing the emulation includes emulating the program instructions that comprise the emulation extension.

As per claim 15, due to the similarity of claim 3 to claim 1 above, and the security enhancement for program code execution in Bond above implies the claimed feature of malicious behavior because the security program in Bond is to enhance program execution by preventing security breaches (col. 2, lines 7-14, for example), uncertainty provenance or effects (col. 4, lines 54-57). In other words, the security enhancement program in Bond is to detect malicious behavior of the suspect code execution in the system and malicious code extent.

As per claim 17, Bond discloses emulating the suspect code prior to loading the emulation extension into the emulator buffer (col. 4, lines 39-57, col. 5, lines 23-33).

As per claims 18-24, Bond discloses the claimed limitations for detecting and preventing malicious codes or security breach in execution of the suspect code.

As per claim 25, Bond discloses a method and a system for security enhancement of untrusted code execution with feature limitations very similar to the claimed invention. According to Bond, the system for security enhancement of suspect code execution includes means:

Receiving the suspect code for execution (col. 5, lines 5-33

Loading the suspect code into an emulation buffer (Fig. 4) within a data space of a computer system,

Loading a first emulation extension into the emulator, wherein the emulator extension including program instruction to emulate suspect code in order to detect a computer virus or malicious software (col. 6, lines 24-52),

Performing an emulation using the first emulation extension and the suspect code, the emulation being performed within an insulated environment in the computer system (Figs 2, 3, col. 6, line 53 to col. 7, line 5) so that the computer system is insulated from malicious actions of the suspect code, and detecting and preventing the system from executing programs containing untrusted code (Field of the Invention). Bond does not expressly disclose the claimed feature of exhibit malicious behavior of the suspect code execution.

It would have been obvious for those skilled in the art at the time of the invention was made to realize the security enhancement in Bond above implies the claimed feature of malicious behaviour because the security program execution in Bond is to enhance program execution by preventing security breaches (col. 2, lines 7-14, for example). In other words, the security enhancement program in Bond is to detect malicious behavior of the suspect code execution in the system.

As per claims 26 and 28, Bond discloses step of performing the emulation includes emulating the program instructions that comprise the emulation extension as claimed.

As per claim 27, due to the similarity of claim 27 to claim 25 above, and the security enhancement in Bond above implies the claimed feature of malicious behaviour because the security program in Bond is to enhance program execution by preventing security breaches (col. 2, lines 7-14, for example) or uncertainty provenance or effects (col. 4, lines 54-57). In other words, the security enhancement program in Bond is to detect malicious behavior of the suspect code execution in the system.

As per claim 29, Bond discloses emulating the suspect code prior to loading the emulation extension into the emulator buffer (col. 4, lines 39-57, col. 5, lines 23-33).

As per claim 30, Bond discloses the claimed limitations for detecting and preventing malicious codes or security breach in execution of the suspect code.

As per claim 31 Bond discloses a plurality of emulation extension for detecting malicious or virus code (Figs. 2-4). This would imply the claimed limitation of resolving conflict.

As per claims 32-36, Bond discloses the claimed limitations for detecting and preventing malicious codes or security breach to resolve conflict and uncertainty provenance of program execution.

Conclusion

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US patent no. 5,619,698, issued to Lilich et al, on Apr. 1997
2. US patent no. 6,014,702, issued to King et al, on Jan. 2000
3. US patent no. 6,035,405, issued to Gage et al, on Mar. 2000
4. US patent no. 6,112,304, issued to Clawson, James, on Aug. 2000
5. US patent application no. US 2003/0177485 A1, issued to Waldin et al, on Sept. 2003

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thai Q. Phan whose telephone number is 703-305-3812.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jean Homere can be reached on 703-308-6647. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

3. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Sept. 28, 2004

Thai Phan
Patent Examiner
Art Unit 2128